Instituto Superior de Economia e Gestão

UNIVERSIDADE TÉCNICA DE LISBOA

DESDE 1911

MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

DISSERTAÇÃO

PRIVACIDADE DE INFORMAÇÃO E A REFORMA DAS DIRETIVAS EUROPEIAS DE PRIVACIDADE DE DADOS

BRUNO MANUEL DIAS CAETANO MARQUES

SETEMBRO 2012

MESTRADO EM
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO

PRIVACIDADE DE INFORMAÇÃO E A REFORMA DAS DIRETIVAS EUROPEIAS DE PRIVACIDADE DE DADOS

BRUNO MANUEL DIAS CAETANO MARQUES

ORIENTAÇÃO:
PROF. DOUTOR MÁRIO MACIEL CALDEIRA
MESTRE BRUNO ARMINDO MACEDO

SETEMBRO 2012

Sumário

A privacidade de informação parece ser, atualmente, uma preocupação crescente para os utilizadores de sistemas de informação (SI), dado o desconhecimento da forma como os seus dados privados são utilizados, por quem, com que intuito e qual a sua fiabilidade. Segundo um estudo recente do Eurobarómetro, os cidadãos europeus encontram-se apreensivos quanto à utilização dos seus dados privados pelas organizações, com especial incidência nas redes sociais e motores de pesquisa, na Internet. A maioria dos utilizadores tem consciência de que o seu conhecimento é reduzido quanto à utilização que é dada aos seus dados privados e de que poderá não ter meios para os controlar quando os colocam diretamente na Internet ou em sistemas de informação, *Web* 2.0, de organizações às quais disponibilizaram dados, estando estes alojados no modelo de *cloud computing*. Vindo ao encontro destas preocupações e necessidades a Comissão Europeia, apresentou uma proposta de novas regras de privacidade de dados que acompanhem estes novos desafios lançados pelo rápido desenvolvimento das tecnologias de informação, orientadas à Internet e à *cloud*, e à necessidade de proteger a privacidade dos dados dos utilizadores. Esta investigação irá estudar os fatores que poderão inibir as organizações de se adaptarem a esta nova necessidade e às novas regras europeias de proteção da privacidade de dados, através do estudo desenvolvido por Bélanger & Crossler (2011) relativo à *Data Privacy Framework* europeia.

Palavras-chave: privacidade de informação, *cloud computing, Web* 2.0

Abstract

Information Privacy seems to be, in nowadays, an increasing concern for information systems users who don't have knowledge about how their information is handled, by whom and with what purpose and accuracy. According to a recent study of the Eurobarometer european citizens find themselves apprehensive when concerning the use of their personal data by organizations, especially social networks and search engines in the Internet. Most users are aware that their knowledge about the use their private data is limited and that might not be able to control their personal data that is used on the Internet or in Information Systems of organizations that host their data in the cloud. Coming to meet these concerns and needs, the European Commission presented new data privacy rules that meet these new challenges posed by the rapid development of information technologies, targeted to the Internet and cloud, and to the need to protect the user data privacy. This research will study the factors that might inhibit organizations from adapting to this need and to the new european data privacy protection rules, through a study developed by Bélanger & Crossler (2011) regarding the european Data Privacy Framework.

Keywords: information privacy, cloud computing, Web 2.0

A. Agradecimentos

Os meus agradecimentos à Vera, ao António e restante família pelo apoio, incondicional, aos orientadores, pela confiança dada e suporte prestado, e aos entrevistados pela partilha da sua experiência e pelo contributo fundamental para realização deste trabalho.

B. Glossário de termos e abreviaturas

CE - Comissão Europeia

DEPD – Diretiva europeia de privacidade de dados

ENISA – European Network and Information Security Agency

IaaS – *Infrastructure-as-a-Service*

IP – *Internet Protocol*

PaaS – *Platform-as-a-Service*

RDIS – Rede digital com integração de Serviços

SaaS – *Software-as-a-Service*

SI – Sistemas de Informação

TI – Tecnologias de Informação

UE – União Europeia

VPN – *Virtual Private Network*

WWW – *World Wide Web*

C. Indice de Figuras

Índice

1. INTRODUÇÃO

A segurança de informação e de dados privados tem sido uma preocupação crescente nos últimos anos, derivado do grande desenvolvimento das tecnologias da informação e aumento da sua utilização (Bélanger & Crossler, 2011). De acordo com um estudo recente, os utilizadores têm cada vez mais consciência do rasto, aqui definido como conjunto de dados privados espalhados por diversos serviços, que deixam na Internet ao colocarem dados privados *online* mas tendo ausente os limites da extensão desse rasto (Madden, Fox, Smith, & Vitak, 2007). Um outro estudo da Comissão Europeia (2011) diz que apesar das preocupações que os utilizadores europeus têm em colocar informação pessoal às organizações que disponibilizam ou processam dados na Internet, três em cada quatro europeus aceita esta disponibilização como fazendo parte do seu dia-a-dia. Este estudo da Comissão Europeia fornece, ainda, mais alguns dados importantes como 62% dos utilizadores europeus fornece apenas os dados mínimos indispensáveis de modo a proteger a sua identidade, que três em cada quatro utilizadores quer que seja possível eliminar as suas contas *online* e os seus registos por completo sempre que assim o desejarem e que essa possibilidade, os seus direitos e as regras sejam iguais por toda a Europa. Um outro estudo, da Agência Europeia para a Segurança da Rede e da Informação (ENISA) afirma que a maioria das empresas europeias recolhe informação privada dos utilizadores considerando esta como um bem que poderá usar para retirar benefícios comerciais (European Network and Information Security Agency, 2012). Ainda neste estudo, metade das empresas admite que armazena informação dos utilizadores para criação de perfis com o objetivo de premeditar comportamentos destes para fins

comerciais, nunca eliminando a respetiva informação após a utilização legítima para o qual foi recolhida.

Em 1995, a União Europeia (EU) criou a Diretiva Europeia de Privacidade de Dados (DEPD), que protege o direito fundamental da privacidade dos cidadãos europeus na Europa. Com a evolução da Internet, e com recurso a inquéritos como o mencionado no parágrafo anterior, a UE decidiu rever as suas regras de privacidade de dados para que estas se ajustem à nova realidade dos serviços disponibilizados na Internet e para que os utilizadores europeus vejam os seus dados privados protegidos independentemente do país onde estes são processados ou guardados. Com a globalização de serviços na Internet, a proteção dos dados privados tornou-se uma necessidade que estas regras prevaleçam fora da Europa, uma vez que os dados poderão estar fora da UE (Comissão Europeia, 2010). Esta revisão, terá maior incidência sobre os serviços, prestados na UE, de *cloud computing* e Web 2.0, conceitos estes que serão apresentados, com maior detalhe, mais adiante neste documento. Estas novas regras deverão obrigar a que os prestadores de serviços possam, apenas, com a respetiva autorização dos utilizadores, divulgar, partilhar e disponibilizar os seus dados pessoais a outras entidades. A nova *Data Privacy Framework* irá, ainda permitir que os utilizadores saibam o que está a ser feito com os seus dados e permitir que estes sejam transferidos para outros serviços (Comissão Europeia, 2012). Deste modo, a UE apresenta na sua proposta para a atualização da sua *framework* de privacidade de dados, alguns objetivos principais tais como: o fortalecimento dos direitos individuais que estabelece que o uso dos dados deverá ser reduzido ao mínimo necessário, com acordo do utilizador após ser esclarecido da forma como e onde os seus dados serão usados; o estabelecimento de regras únicas

para a privacidade dos dados dos utilizadores da UE; o acesso das agências de segurança e da justiça aos dados privados; a prevalência das regras europeias quando os dados são armazenados ou processados fora da zona europeia; e por fim assegurar que estas regras são aplicadas e não são quebradas (Comissão Europeia, 2010).

A investigação aqui proposta, pretende, com base na nova DEPD, estudar os fatores que poderão inibir a adoção das novas regras de privacidade de dados da UE pelas organizações, com base em alguns casos de organizações portuguesas, de setores de atividade diferentes entre si. Este estudo irá verificar, assim, se as organizações portuguesas têm forma de proteger os dados, colocados em sistemas de informação alojados em *cloud computing* e em aplicações *Web* 2.0, dos cidadãos europeus, e os fatores que poderão inibir as próprias organizações no processo de implementação destas mesmas regras.

A Revisão Bibliográfica irá fornecer fontes, com diversos pontos de vista e formas de analisar a segurança de dados privados que poderão ser aplicados neste estudo da aplicação da *Data Privacy Framework* a ser desenvolvida pela Comunidade Europeia.

1.1. Motivação

Para o investigador este tema, tem especial interesse pela sua atualidade, dado que as novas regras europeias foram propostas em Janeiro de 2012 e se encontram em avaliação pelos estados-membros. Também, o baixo número de estudos na área e crescente preocupação dos cidadãos europeus (Bélanger & Crossler, 2011), a aplicação, a nível europeu, das regras e sua repercussão mundial, bem como as áreas que são implicadas pela aplicação da nova *Data Privacy Framework* levam o

investigador a acreditar que este estudo venha a servir os interesses tanto da comunidade académica como dos profissionais da área de sistemas de informação.

Por forma a contextualizar o estudo serão apresentados, de seguida, os conceitos de base que o sustentam.

2. CLOUD COMPUTING

O *Cloud Computing* surge como um novo modelo de computação distribuída, para clientes empresariais ou individuais que disponibiliza recursos de *hardware* e *software,* em *data centers* remotos e públicos, pagando as organizações, pelos serviços, apenas os recursos que utilizar (Chen & Wang, 2011). Esta nova solução de utilização de *hardware* e *software* permite que os meios necessários, para determinado projeto, sejam adquiridos ou contratados à medida das necessidades do mesmo, e alterados ao longo do tempo consoante a variação dos recursos necessários para o funcionamento do mesmo (Armbrust, et al., 2010). Esta plataforma de serviços de *hardware* e *software* pode surgir em três modelos distintos: o primeiro, como disponibilização de recursos de *hardware* à medida para o cliente, *Infrastructure-as-a-Service* (IaaS), através da virtualização de infra-estruturas tendo como exemplo as máquinas virtuais (Takabi, Joshi, & Ahn, 2010); o segundo como disponibilização de plataformas de serviço para o cliente, como exemplo surgem os sistemas de gestão de bases de dados ou servidores aplicacionais e que poderão dar suporte a ambientes de desenvolvimento (Takabi, Joshi, & Ahn, 2010), *Platform-as-a-Service* (PaaS); o terceiro e último será a disponibilização de serviços de *software* à medida das necessidades, como exemplo surgem os *softwares* de CRM, ERP ou colaborativos tais como editores de texto ou folhas de cálculo, Software-as-a-Service (SaaS) (Armbrust, et al., 2010)

(Takabi, Joshi, & Ahn, 2010). Um estudo efetuado nos Estados Unidos da América, revela que 69% dos americanos já utiliza aplicações em *cloud computing* (Soghoian, 2009). Nestes três modelos, o nível de segurança que deverá ser fornecido pelo prestador do serviço diminui à medida que aumenta o nível de abstração do serviço, sendo IaaS que contém o nível mais elevado, seguindo-se o PaaS e finalmente o SaaS. No sentido contrário, o nível de segurança e proteção quanto aos dados que deverá ser prestado pelo cliente do serviço é maior quanto maior for o nível de abstração do modelo em uso. Assim no caso de utilização em SaaS terá que ter um nível maior de segurança por parte do cliente do serviço de *cloud computing*, diminuindo no modelo de PaaS e sendo o menor nível em IaaS (Takabi, Joshi, & Ahn, 2010).

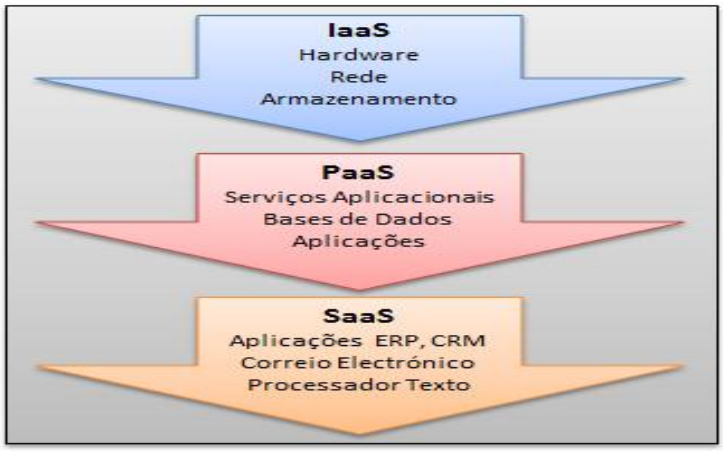

Ilustração 1 - Utilização de recursos TI em Cloud (adaptado de Toal (2011))

No entanto, o *Cloud Computing* apesar de apresentar soluções potencialmente vantajosas para utilização de recursos e serviços de tecnologias de informação, deixa, ainda, em aberto algumas questões de segurança e privacidade (Chen & Wang, 2011). A aplicação de regras de proteção e privacidade num modelo de *cloud computing* poderá ser complexo e de difícil aplicação, uma vez que os requisitos de segurança e privacidade irão certamente variar de cliente para cliente e de sistema para sistema (Takabi, Joshi, & Ahn, 2010). Outra questão importante é o armazenamento de dados

numa infra-estrutura partilhada por mais do que um cliente o que poderá levantar problemas de acesso não autorizado (Takabi, Joshi, & Ahn, 2010) sendo necessário que o prestador de serviço de *cloud computing* garanta a confidencialidade, integridade e disponibilidade dos dados (Harauz, Kaufman, & Potter, 2009).

O uso de *cloud computing* oferece algumas vantagens adicionais aos prestadores de serviços de *cloud computing*, tais como facilidade no controlo de acessos, proteção da tecnologia utilizada, quer seja a nível de *hardware* quer a nível de *software*, e segurança. Para os clientes, organizações utilizadoras do serviço, é garantida a utilização da última versão do *software*, em serviços SaaS, independência do computador com que se acede ao serviço (Soghoian, 2009).

Do lado das desvantagens, o uso de tecnologia de *cloud computing* permite uma maior abertura à invasão de privacidade dos utilizadores e a acessos indevidos (Soghoian, 2009). Os riscos associados a esta exposição não são muitas vezes comunicados aos utilizadores, impedindo que estes tomem decisões informadas sobre a utilização dos mesmos. Além destas desvantagens, existe ainda a ausência de preocupação, de muitos prestadores de serviços, com a segurança destes mesmos serviços dado que não existe exigência do mercado. O desconhecimento dos utilizadores quanto à segurança e vulnerabilidades existentes, a que estão sujeitos neste tipo de serviços, fomenta este tipo de comportamento. (Soghoian, 2009).

O *cloud computing* dá, assim, origem a que as organizações utilizem *hardware* e software baseado em tecnologia distribuída na *cloud* o que significa que os dados dos seus clientes estarão dispersados geograficamente. As tecnologias *cloud* são, hoje em dia, um recurso utilizado para os serviços *Web* 2.0 que apresentamos de seguida.

3. *WEB* 2.0

A *Web* 2.0 é um conceito que surge em 2004, e que define a *Web* como uma plataforma para serviços, não só para a Internet, mas também para todas as pessoas, com integração dos mais diversos dispositivos que com elas estejam relacionados de forma segura (Kormaris & Spruit, 2010), revolucionando o modo como é feito o negócio pelas organizações (Lee, Kim, Noh, & Lee, 2010). A versão *Web* 2.0 apresenta a adição de conteúdos por parte dos utilizadores como fator de diferenciação da versão anterior. Esta possibilidade proporciona uma maior interatividade social, possibilitando a partilha de informação e a comunicação entre pessoas na *Web* (Boulos & Wheeler, 2007). Alguns exemplos de serviços disponibilizados, na plataforma *Web* 2.0, são as redes sociais como o Facebook, LinkedIn ou Google+, serviços comerciais como a Amazon ou E-Bay, ou os motores de pesquisa, como o Google ou Bing, e os *blogs*. A conetividade proporcionada por esta nova plataforma de serviços *Web*, proporcionou um maior relacionamento entre as pessoas que utilizam os mesmos serviços e ao mesmo tempo, a partilha de dados pessoais disponibilizados nesses mesmos serviços (Musser, 2006). Assim, para além da obtenção de conhecimento a partir da Internet, os utilizadores podem partilhar o seu próprio conhecimento de forma fácil e intuitiva. Esta possibilidade de interação, proporcionada pela *Web* 2.0, contribuiu para o aumento do uso das tecnologias de informação nos últimos anos (Boulos & Wheeler, 2007).

Devido ao aumento da utilização da Internet e das tecnologias de informação e da sua evolução, os serviços *Web* 2.0 ganham importância no mercado, sendo uma das indústrias com maior poder económico nos Estados Unidas da América e na Europa

(Soghoian, 2009). Este tipo de serviços, incentivam os utilizadores a adicionar conteúdos e dados pessoais, sendo estes controlados pelos próprios utilizadores. Estes conteúdos e dados pessoais podem ser partilhados, referenciados e pesquisados quer por outros utilizadores quer por outros serviços *Web* 2.0 (Lee, Kim, Noh, & Lee, 2010).

Muitos dos serviços *Web* 2.0 onde são depositados dados privados e conteúdos partilhados pelos utilizadores são alvo de acesso pelos motores de pesquisa. Estes motores processam e indexam todo o conteúdo disponibilizado e acessível nos serviços públicos como por exemplo as redes sociais, *wikis* e *blogs*. Assim, reunindo informação de diversas fontes de um determinado utilizador, sem que este se aperceba, e sem autorização explícita, os motores de pesquisa conseguem, posteriormente, analisar os dados recolhidos, tais como histórico de navegação, endereços IP, perfis de redes sociais entre outros e traçar perfis dos utilizadores. Com os dados recolhidos e com os perfis traçados, os motores de busca conseguem assim disponibilizar serviços de informação que podem ser disponibilizados aos próprios utentes ou a terceiros. A sugestão de páginas de internet com base no histórico e na localização do utilizador, é um dos casos de serviço disponibilizado ao próprio utilizador quando este efectua uma pesquisa no motor. Estes serviços poderão, também, ser dirigidos, para efeitos de marketing, a organizações que queiram direcionar a publicidade dos seus produtos a utilizadores que sejam mais propensos ao seu consumo com base nos perfis fornecidos. Esta publicidade pode surgir na forma de resultado de uma pesquisa efectuada, surgindo um produto adequado ao perfil do utilizador no topo de resultados da pesquisa ou ser direccionada e apresentada noutros serviços *Web* 2.0, tais como as redes sociais. Por outro lado, os dados recolhidos poderão ser utilizados por forças de segurança ou governamentais para

efeitos de investigação ao próprio ou ainda a outros utilizadores com outras intenções. O tipo de integração, aqui descrita, entre os serviços *Web* 2.0 e os motores de pesquisa é aplicado o nome de *Search* 2.0 (Zimmer, 2008).

No entanto, é neste tipo de serviços, *Web* 2.0, que os utilizadores depositam os seus dados privados sem que na maioria das situações tenham conhecimento da localização em que são colocados ou com quem são partilhados. Os utilizadores são assim expostos a possíveis riscos de invasão de privacidade sem terem o conhecimento da sua situação (Soghoian, 2009). No caso de uso dos dados fornecidos por plataformas *Search* 2.0, e apesar de os conteúdos disponibilizados serem recolhidos de localizações públicas, na Internet, a criação de perfis com base nesses conteúdos e derivados da própria navegação, na Internet, levantam questões de privacidade de informação dos utilizadores uma vez que podem ser registados, para além dos supracitados perfis traçados, quaisquer comportamentos que os utilizadores tenham quer na navegação quer noutras circunstâncias e tenham sido publicados (Zimmer, 2008). Este tipo de processamento, de informação dos utilizadores, e as outras aplicações dadas, anteriormente citadas, remetem-nos para o conceito de Privacidade de informação que abordaremos de seguida.

4. PRIVACIDADE DE INFORMAÇÃO

Atualmente, a preocupação que é dada, pelos utilizadores, ao uso que é feito dos seus dados pessoais, por si disponibilizados nas aplicações *web*, é cada vez maior (Bélanger & Crossler, 2011). Os serviços *web* interagem cada vez mais entre si, recolhendo, desta forma, dados que não são disponibilizados diretamente pelos utilizadores mas sim pelas próprias aplicações sem que os utilizadores tenham dado o

seu consentimento ou que tenham consciência de que esta partilha está a ser efetuada. Neste sentido as redes sociais são o caso mais notório de partilha de informação. Os utilizadores preenchem os seus perfis com dados pessoais que posteriormente podem ser disponibilizados a terceiros para outros efeitos que não os inicialmente pensados pelo utilizador. Noutra perspetiva, com o crescente uso do *cloud computing*, os serviços que colocam os seus dados armazenados na *cloud* terão que garantir aos utilizadores que os seus dados se encontram seguros e que não serão alvo de perda ou de acesso indevido. Assim, surge a privacidade de informação como meio de controlo de acesso, de utilização e manutenção de dados pessoais.

A privacidade de informação pode ser definida de variadas formas tendo, até, sido alvo de diversos estudos (Bélanger & Crossler, 2011) mas que nos dias de hoje começa a ter mais atenção na pegada que os utilizadores deixam na Internet através da partilha dos seus dados pessoais e de navegação na própria Internet. Alguns autores apresentam a privacidade de informação como sendo a capacidade dos utilizadores controlarem de que forma são utilizados e por quem são utilizados os seus dados armazenados em aplicações *web* ou armazenados na *cloud* por prestadores de serviços, na Internet (Bélanger & Crossler, 2011). A privacidade de informação pode ser avaliada em quatro pontos: a privfacidade que define qual o nível de privacidade dos dados; fiabilidade que verifica se os dados estão correctos e são verdadeiros; propriedade que valida o proprietário dos dados; e por fim, a acessibilidade que define quem pode aceder aos dados. Nos dias de hoje, começa-se a ter mais atenção na pegada que os utilizadores deixam na Internet. Segundo um estudo, a consciencialização dos utilizadores começa a aumentar relativamente a este assunto (Madden, Fox, Smith, & Vitak, 2007). Os utilizadores verificam que os seus dados são

partilhados entre diversos sistemas sem que tivessem dado consentimento para tal. Consciente destas situações, a Comunidade Europeia, desenvolveu uma nova *Data Privacy Framework*, conjunto de regras de utilização de dados privados, apresentada em Janeiro de 2012, partindo da original datada de 1995, de forma a proteger os cidadãos europeus (Comissão Europeia, 2010) e que se encontra em avaliação pelos estados-membros da UE.

A segurança de informação privada tem vindo a ter cada vez mais o foco por parte das organizações, com o aumento da utilização de sistemas de informação (Bélanger & Crossler, 2011), levando os custos que as organizações têm tido com a segurança de informação a crescer, ao longo dos últimos anos (Dhillon, 2004). A privacidade de informação pode ser definida de variadas formas tendo até sido alvo de diversos estudos (Bélanger & Crossler, 2011).

Partindo do estudo de Bélanger & Crossler (2011) que avalia o estado da privacidade de dados nos Estados Unidos da América, esta investigação conjugará, esse mesmo estudo, com as propostas de *Data Privacy Framework* que a União Europeia se encontra a desenvolver. Será avaliada a literatura que mostre o estado e a preocupação atuais, das organizações portuguesas, para esta temática e, partir desse ponto, para avaliar a capacidade de implementação da nova *framework*, os beneficios e prejuizos que possa trazer, e a forma como serão utilizados os dados. Será necessário identificar uma estratégia, de classificação de privacidade de dados, que permita identificar niveis para a sensibilidade e confidencialidade dos dados, onde serão estes guardados e de que modo serão acedidos (Tumulak, 2010).

5. DIRETIVAS EUROPEIAS DE PROTEÇÃO DE DADOS

O objetivo da DEPD é a regulamentação das políticas de privacidade de informação nos países membros da UE. Com a uniformização das leis, nos países pertencentes à UE, a circulação de informação privada dos cidadãos europeus será tratada da mesma forma em todos os países membros, quer seja por um processo automático ou por um processo manual.

A utilização de informação privada deverá sempre respeitar os três critérios base da diretiva: a transparência, o propósito legítimo e a proporcionalidade (Kosta, Dumortier, & Graux, 2012) (Comissão Europeia, 1995). A transparência refere-se ao direito que um individuo tem de ser informado pelo utilizador dos seus dados de que irá ocorrer um processamento sobre estes, a razão desse processamento, qual o destino desse processamento e em que condições é efetuado esse mesmo processamento. O propósito legítimo indica se a razão do processamento e a extensão da utilização dos dados se enquadram nos limites legítimos e propostos inicialmente. A proporcionalidade remete-nos para a precisão da informação e para a validade dos dados tendo em conta o propósito para o qual foram recolhidos. Sempre que necessário para o objetivo final, os dados devem ser retificados e atualizados. Ainda para finalizar, o critério da proporcionalidade, deve verificar a utilização dos dados para efeitos de histórico, processamentos estatísticos ou científicos. Assim, o critério da proporcionalidade irá garantir que serão utilizados apenas os dados estritamente necessários, apenas na duração necessária para o processamento dos dados acordada pelo utilizador ou até este cancelar a autorização para o processamento desses mesmos dados (Kosta, Dumortier, & Graux, 2012).

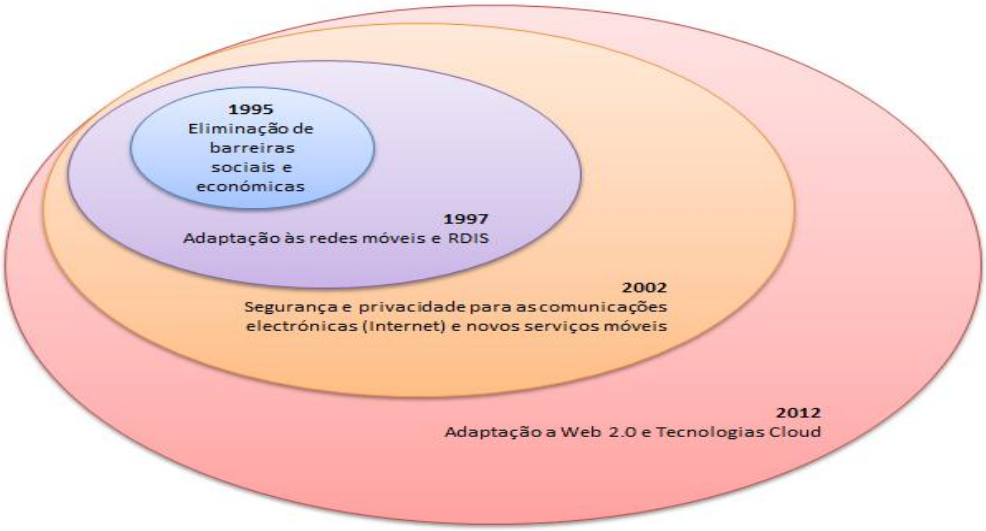

Ilustração 2 - Evolução da directiva europeia e das TI

5.1. CONCEITOS

Anteriormente à apresentação das diretivas, serão expostos alguns conceitos, referenciados nas diretivas, que permitem um melhor entendimento das mesmas:

- Dados Pessoais - são qualquer informação relativa a uma pessoa singular identificada ou identificável, direta ou indiretamente, pelos dados disponibilizados (Comissão Europeia, 1995).

- Tratamento de dados – é qualquer operação ou conjunto de operações efetuadas sobre os dados pessoais, de forma automática ou manual, tais como a recolha, registo, organização, conservação, adaptação, alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão, disponibilização, bloqueio, apagamento ou destruição (Comissão Europeia, 1995).

- Consentimento da pessoa - qualquer manifestação de vontade, livre, especifica e informada, pela qual a pessoa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento (Comissão Europeia, 1995).

- Utilizador - Pessoa singular que utilize o serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante deste serviço (Comissão Europeia, 2002).

- Dados de Trafego - quaisquer dados tratados, para efeitos de envio, de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos de faturação da mesma (Comissão Europeia, 2002).

5.2. A DIRETIVA DE 1995

A diretiva 95/46/CE do parlamento europeu e do conselho de 24 de Outubro de 1995 foi criada com o objetivo de gerar mais e maiores relações sociais económicas de todos os estados pertencentes à UE eliminando barreiras impeditivas destas relações (Comissão Europeia, 1995). Com esta diretiva, os dados pessoais dos cidadãos europeus, independentemente da sua nacionalidade ou residência, podem circular livremente entre estados-membro, preservando e protegendo os direitos fundamentais das pessoas. A equivalência do tratamento de dados pessoais por todos os Estados-membros permite que os princípios de proteção de dados sejam aplicados e regidos pelo direito comunitário. A diretiva considera que os princípios de proteção são aplicáveis a toda e qualquer informação. Esta directiva, 95/46/CE, pretende, ainda, eliminar barreiras que diferentes legislações dos Estados-membros possam ter que venham a interferir com atividades económicas, entre estados-membros, eliminando essas diferenças e conferindo uma igualdade tanto a nível de direitos como de privacidade e segurança aos dados pessoais em circulação (Comissão Europeia, 1995). Estes princípios de proteção deverão ser aplicados, com excepção de processamentos de dados efectuados por pessoas singulares em actividades pessoais, a todos os processamentos e atividades regidas pelo direito dos estados-membros da UE.

Os princípios da proteção de dados são aplicáveis, a qualquer informação, que possa revelar quem é o seu dono, quer esta informação sofra um tratamento automatizado ou manual, impedindo, assim, a possibilidade de contornar a protecção conferida à informação, devido à forma como é efetuado o tratamento de dados. O tratamento de dados, independentemente de ser executado de forma automática ou manual, deve ser efetuado de forma licita, adequada, sem tratamento excessivo que ultrapasse os objetivos para o qual foram inicialmente disponibilizados, devendo estes objetivos ser claros, explícitos e legítimos e disponibilizados ao utilizador no momento do pedido de disponibilização destes (Comissão Europeia, 1995).

Esta diretiva, não se aplica a operações realizadas sobre os dados pessoais não sujeitas ao direito comunitário ou a operações que tenham como objectivo a segurança pública, defesa e segurança dos Estados-membros ou, ainda, operações realizadas por uma pessoa singular no decorrer de atividades exclusivamente pessoais ou domésticas (Comissão Europeia, 1995).

Os princípios relativos à qualidade dos dados devem ser: tratamento leal e lícito, com finalidades e objetivos bem definidos e pré-determinados sendo que o tratamento para efeitos de histórico é possível desde que sejam assegurados todos os princípios de privacidade; dados adequados e não excessivos para a finalidade proposta e tratamento posterior; exactos e atualizados, sempre que necessário ou seja pertinente; e conservados apenas pelo período estritamente necessário para cumprir a finalidade para o qual foram recolhidos (Comissão Europeia, 1995).

Por fim, esta diretiva deverá garantir que os donos dos dados têm da parte da entidade responsável pelo processamento as seguintes condições: o acesso livre e sem

restrições, dentro de um período razoável e sem custos excessivos aos seus dados; se os seus dados foram ou não tratados, para que fim foi efetuado esse tratamento e para que destinatários; qual a origem dos dados e que tratamento foi efetuado sobre estes quer tenha sido de forma automatizada ou não; a garantia que sejam colocadas em prática as medidas necessárias à segurança e proteção dos dados pessoais; a confidencialidade dos dados pessoais (Comissão Europeia, 1995).

5.3. A REVISÃO DE 1997

A diretiva 97/66/CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações estendeu a regulação da privacidade de dados da diretiva de 1995 ao setor das telecomunicações (Comissão Europeia, 2002). Esta diretiva, visava, à data, a evolução que estava a ser introduzida nas redes de telecomunicações através de tecnologias digitais avançadas, nomeadamente a Rede Digital Integrada de Serviços (RDIS) e redes móveis (Comissão Europeia, 1997).

Esta diretiva, pretende garantir a confidencialidade das comunicações efectuadas pelas redes públicas e pelos serviços de telecomunicações. Tal confidencialidade abrange a proibição de escutas, gravação e armazenamento de comunicações sem o consentimento dos utilizadores, a possibilidade de apresentação e restrição de identificação da linha chamadora e da linha conectada (Comissão Europeia, 1997).

5.4. A REVISÃO DE 2002

A diretiva 2002/58/CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas tem como objectivo a regulação do tratamento, segurança e privacidade no setor das comunicações electrónicas nos Estados-membros da UE, transpondo os princípios estabelecidos na diretiva de 95 e revogando a directiva de 97, relativamente ao setor das telecomunicações que

deverão ser actualizadas devido à introdução de novas tecnologias e serviços de comunicações eletrónicas proporcionando um nível de segurança e privacidade aos utilizadores destes, independentemente da tecnologia utilizada (Comissão Europeia, 2002).

5.5. A ACTUAL REVISÃO DA DIRETIVA EUROPEIA

Em 2010, para fazer face à crescente utilização da Internet e desenvolvimento das tecnologias *cloud* e *Web* 2.0, a Comissão Europeia decidiu rever e actualizar a diretiva de 1995 de modo a proteger a privacidade da informação disponibilizada pelos cidadãos europeus (Comissão Europeia, 2010). Este novo conjunto de regras, *Data Privacy Framework*, procurará ter implicações ao nível dos sistemas de informação e da actual *Data Privacy Framework europeia*, permitindo que os cidadãos europeus possam controlar e apagar a totalidade dos seus registos, sem que estes fiquem perdidos nas sucessivas partilhas de dados entre diferentes sistemas de informação (Comissão Europeia, 2011). Esta proposta, vem ao encontro tanto das necessidades dos cidadãos europeus no que respeita ao controlo sobre os seus próprios dados, necessidades estas reveladas pelo estudo realizado pelo Eurobarómetro/Comissão Europeia em 2010, bem como pela percepção da realidade actual, no que se refere à utilização sem consentimento e para além do propósito legítimo dos dados privados dos utilizadores, das organizações com base no estudo da ENISA realizado em 2012.

Com esta nova proposta, os titulares dos dados têm o direito a serem esquecidos e a que os seus registos sejam eliminados pela entidade responsável pelo processamento. Este direito deverá ser aplicado sempre que se verifique que os dados deixaram de ser necessários para o objetivo para o qual foram disponibilizados

inicialmente, ou que o titular dos dados retire a autorização para o tratamento ou disponibilização dos mesmos, ou quando a entidade tratadora dos dados perca a necessidade de ter em sua posse os dados ou o prazo de utilização tenha expirado (Comissão Europeia, 2012).

Esta proposta, reserva, também, o direito do titular dos dados de obter a cópia dos seus dados, da entidade responsável pelo tratamento, de modo a que estes dados possam ser reutilizados pelo titular (Comissão Europeia, 2012).

6. REVISÃO BIBLIOGRÁFICA

Apesar da atualidade do tema, estando neste momento a ser avaliada a proposta de actualização da DEPD, não existem muitos estudos sobre a privacidade de informação e segurança de dados em ambientes de *cloud computing* e *Web* 2.0 (Bélanger & Crossler, 2011).

Bélanger & Crossler (2011) apresentam uma revisão de literatura onde apresentam as principais preocupações de privacidade e segurança na perspetiva dos utilizadores da Internet, com maior incidência em sistemas Web 2.0, onde são colocados dados privados.

Para contextualização do estado da legislação europeia relativa à privacidade de dados, é apresentado em Comissão Europeia (1995), a DEPD original e em Comissão Europeia (1997) e Comissão Europeia (2002) são apresentadas as revisões consequentes da primeira diretiva.

Comissão Europeia (2012) apresenta a proposta de atualização da DEPD que serve de base de análise para o estudo que está a ser apresentado neste documento. Nesta

proposta são apresentados todos os pontos a atualizar, no que respeita à privacidade de dados dos cidadão europeus, dos quais são destacados os seguintes:

- Direito ao apagamento completo da informação privada;

- Direito à obtenção de cópia da totalidade dos dados, em formato "legível";

- Utilização de dados privados apenas com consentimento do dono dos mesmos

- Utilização dos dados mínimos necessários e pelo tempo máximo necessário para o processamento dos mesmos.

Para contextualização tecnológica, do conceito de *cloud computing* no estudo, é apresentada a seguinte literatura Chen, J., & Wang, L. (2011), Armbrust, et al., (2010), Takabi, Joshi, & Ahn, (2010). Soghoian (2009) apresenta vantagens e desvantagens, do *cloud computing,* e as lacunas existentes, no contexto dos Estados Unidas da America, quanto à privacidade de informação.

Relativamente à *Web* 2.0, Kormaris & Spruit, (2010) e Lee, Kim, Noh, & Lee, (2010) apresentam o próprio conceito de *Web* 2.0 complementado por Boulos & Wheeler, (2007) e Musser, (2006) com a apresentação da usabilidade e extensabilidade dos serviços que utilizam este modelo. Soghoian, (2009) fornece informação sobre o nivel de utilização e o impacto na economia do modelo e Zimmer, (2008) apresenta a integração deste modelo com os motores de pesquisa e o respetivo conceito de Search 2.0 e a ligação à principal questão do estudo, a privacidade de informação.

Os estudos analisados sobre a privacidade de dados e as preocupações dos utilizadores são apresentados por Madden, Fox, Smith, & Vitak, (2007) num contexto dos Estados Unidos da América e mais recentemente por Comissão Europeia (2011).

Por outro lado, em ENISA (2012), é apresentado um estudo, realizado pela própria ENISA, que revela o tipo de utilização que é efectuada com dados dos utilizadores pelas organizações dos 27 estados membros da EU.

7. METODOLOGIA

Para o presente estudo foi utilizado um modelo de investigação dividido em quatro fases. A primeira fase apresenta a revisão bibliográfica para a fundamentação teórica do estudo e que se desenvolveu ao longo de toda a elaboração do mesmo. A bibliografia consultada incidiu sobretudo no tema da privacidade de informação em ambientes de *cloud computing* e *Web* 2.0. Alguma da bibliografia apresenta estudos relativos à temática investigada por forma a contextualizar o uso da tecnologia por parte dos utilizadores e dos fornecedores de serviços.

A segunda fase consiste na realização de entrevistas a membros de organizações privadas e publicas com responsabilidade na área do planeamento de sistemas de informação e de segurança de dados e aplicações. Através destas entrevistas serão recolhidos dados sobre o atual estado das organizações quanto à privacidade da informação, qual o nível de preocupação e atenção que esta temática representa para as organizações, qual o impacto que a adoção das novas regras de privacidade de informação poderá causar tanto a nível de sistemas de informação como de negócio, e que fatores poderão, potencialmente, dificultar ou inibir a implementação das novas regras.

Na terceira fase, serão avaliados os dados obtidos nas entrevistas realizadas e, posteriormente, codificados de modo a que seja possível a sua interpretação e integração de maneira a que se possa retirar resultados, para utilização neste estudo.

Na quarta e última fase, serão apresentados os resultados obtidos através do processo de análise às entrevistas efetuadas que permitirão a este estudo apresentar as conclusões finais.

7.1. RECOLHA DE DADOS

A recolha de dados deste estudo irá centrar-se inicialmente na consulta de literatura académica da especialidade, de privacidade de dados e segurança, de tecnologias *cloud computing* e *Web* 2.0, e de documentação técnica da Comissão Europeia relativa à nova *Data Privacy Framework* já apresentada na revisão bibliográfica deste estudo.

Nas entrevistas efetuadas, através das quais foram recolhidos dados, para o estudo de caso, focaram-se os seguintes pontos de análise:

- Preocupações, utilizadores e organizações sobre privacidade de informação

- Estado atual de segurança de dados a nível de SI/TI e na organização;

- Utilização atual de sistemas em *cloud computing* na organização*;*

- Evolução da segurança para *cloud computing* e *Web 2.0* na organização*;*

- Utilização de sistemas Web 2.0 na organização;

- Proposta de atualização da Diretiva Europeia de privacidade de dados;

- Aplicabilidade da nova *Data Privacy Framework* da CE*;*

- Vantagens e desvantagens das novas regras

7.2. QUESTÃO DE INVESTIGAÇÃO

A questão de investigação que este estudo se irá propor a responder será "Que fatores poderão inibir a implementação da nova *Data Privacy Framework* europeia de

privacidade de dados?". Com esta questão irá ser entendido se as organizações dotam de meios para a adoção das novas regras europeias de privacidade de dados, se o seu cumprimento não irá colocar o seu modo de fazer negócio em risco, se os consumidores portugueses conseguirão controlar os seus dados fora destas organizações, e se conseguirão garantir aos consumidores que os seus dados colocados em arquiteturas *cloud* e serviços *Web* 2.0 estão seguros no que respeita a utilização indevida.

7.3. ENTREVISTAS

As entrevistas efetuadas, do tipo não estruturado, com perguntas abertas, foram realizadas a diversos colaboradores de organizações, privadas e públicas, de variados setores de atividade e que têm responsabilidades no que diz respeito a implementação de sistemas de informação, em termos arquitetura e segurança. As entrevistas foram realizadas nas organizações dos entrevistados, tendo uma duração variável entre os trinta minutos e uma hora e vinte minutos. A opção pela diferenciação dos setores de atividade de cada uma das organizações teve como o objetivo o enriquecimento do estudo, com uma visão profunda sobre os fatores inibidores e especificidades de cada setor, mas contendo um caráter abrangente, quanto à utilização das tecnologias mencionadas, *cloud computing* e *Web 2.0.* Foi possível obter dos entrevistados, uma visão direcionada do estudo, obtendo os tais os níveis de preocupação e atenção que são dados à privacidade da informação dos clientes dos seus serviços e daí retirar os fatores inibidores.

O facto de se ter tomado a opção por entrevistas não estruturadas e questões abertas permitiu que os entrevistados contribuíssem, para além dos dados fornecidos relativos às suas empresas quanto à temática deste estudo, com as suas opiniões e

experiência profissional sobre o estado atual, tanto do seu setor atividade como em Portugal, relativos à utilização das tecnologias de *cloud computing* e *Web 2.0* e o seu enquadramento com a privacidade da informação e a recente proposta de atualização da DEPD. Os setores de atividade abrangidos por este estudo são:

- Serviços de TI, tendo sido entrevistado o gestor de negócio e serviços;

- Aviação, tendo sido entrevistado um gestor de TI;

- Saúde Privada, tendo sido entrevistado um gestor de TI;

- Imprensa, tendo sido entrevistado um gestor de TI;

- Serviços de telecomunicações, tendo sido entrevistado o gestor de arquitetura e planeamento tecnológico;

- Serviços *Housing* e *Hosting* de TI, tendo sido entrevistado o diretor de Gestão;

- Serviços Web 2.0, entrevista realizada com arquitecto TI

No anexo A, são apresentadas as principais questões efetuadas nas entrevistas.

7.4. ANÁLISE DE DADOS

Para a análise de dados foi efetuada a codificação das respostas dos entrevistados. Esta codificação surge na forma de três tabelas representativas das respostas sobre o conhecimento e implementação da diretiva europeia de proteção de dados e da sua reforma, sobre a utilização de TI nas organizações e procedimentos internos, e por fim sobre o impacto que a implementação das novas regras terão nas organizações.

Na tabela 1, apresentamos as respostas às seguintes questões:

- "O entrevistado detém conhecimento sobre a DEPD?" em que foi efetuada a codificação com resposta "não" caso o entrevistado não conheça a diretiva ou caso

tenha conhecimento da sua existencia mas não conheça o seu conteudo. A resposta "sim" é colocada se o utilizador para alem de ter conhecimento da existencia da directiva conhecer também parte ou a totalidade do seu conteudo;

- "O entrevistado detém conhecimento sobre a reforma da DEPD?" em que foi efetuada a codificação com resposta "não" caso o entrevistado não conheça a reforma ou caso tenha conhecimento da sua existencia mas não conheça as principais actualizações às regras. A resposta "sim" é colocada se o utilizador para alem de ter conhecimento da existencia do processo de reforma da DEPD, conhecer também parte ou a totalidade das novas regras;

- "É possível a eliminação total dos dados dos utilizadores?" a resposta é codificada em "não" se não for possível a eliminação total ou parcial, em que não seja possivel identificar o utilizador proprietário dos dados. A resposta é codificada em "sim", se for possível eliminar a totalidade dos dados ou no minimo a eliminação parcial de modo a que não seja possível identificar o proprietário pela parte que permanece armazenada;

- "É possível a portabilidade dos dados dos utilizadores?" a resposta é codificada em "não" se não for possível a portabilidade dos dados e em "sim" se for possível;

- "São recolhidos os dados minimos necessários para o processamento?" a resposta é codificada em "não" se forem recolhidos dados adicionais para além dos estritamente necessários para o processamento para o qual o utilizador disponibilizou dados e em "sim" se a recolha for a minima necessária;

- "Os dados, dos utilizadores, recolhidos são armazenados apenas pelo tempo necessário para efetuar o processamento para o qual foram recolhidos?" é codificada em "não" se os dados forem armazenados por tempo indefinido, quer por não existir

procedimento para a eliminação, quer sejam usados posteriormente para outros efeitos como estatisticos ou comerciais, e é codificada em "sim" se os dados forem imediatamente eliminados após o processamento solicitado;

- "Todos os processamentos efetuados sobre os dados dos utilizadores têm o seu consentimento explicito?" é codificada em "não" se existir pelo menos um processamento sobre os dados que esteja fora do ambito do serviço subscrito pelo utilizador e é codificada em "sim" se não existir um ou mais procedimentos que sejam efetuados sem o consentimento dos utilizadores.

Na tabela 2, são apresentadas as codificações relativas às questões sobre o actual estado de utilização de TI por parte das organizações:

- Relativamente à questão "São utilizados recursos internos de TI na organização?" é codificado na resposta "sim" se a organização alojar pelo menos um serviço de TI, com recursos próprios em centros de computação dentro da própria organização, que tenha a possibilidade de ser alojado externamente ou em regime de alojamento externo, *housing,* sem partilha dos recursos com outra organização e em "não" se esse caso não ocorrer;

- "A organização utiliza recursos TI no modelo de *cloud computing*?" é codificado em "sim" se existir pelo menos um serviço, na organização, alojado no modelo de *cloud computing* e em "não" se não existir nenhum serviço neste modelo;

- "A organização presta serviços de *cloud computing*?" é codificado em "sim" se existir pelo menos um serviço, alojado na infra-estrutura de TI da organização, que seja de outra organização e que seja acedida pela internet e em "não" se esta situação não se verificar;

- "A organização utiliza TI *Web* 2.0?" é codificado em "sim" se existir pelo menos um serviço, na organização, que utilize este tipo de serviço e em "não" se não existir;

- "A organização presta serviços de TI *Web* 2.0?" considera a resposta "sim" se for possível receber conteúdos dos utilizadores, externamente à organização e pela Internet, e em não se esta situação não se verificar;

- à questão "A organização partilha conteúdos disponibilizados pelos utilizadores publicamente?" é considerada a resposta com sendo "sim" se os conteúdos inseridos pelos utilizadores, em pelo menos um serviço disponibilizado pela organização, forem publicados e acedíveis pela Internet e em "não" se tal não acontecer;

- a questão "A organização partilha dados dos seus utilizadores com serviços TI de outras organizações?" é considerada resposta "sim" se existir pelo menos um serviço TI, na organização, que disponibilize dados dos utilizadores a outras organizações, quer seja por regras de negócio quer seja para efeitos comerciais, e em "não" se tal não suceder;

- a questão "Quais os tipos de dados partilhados pelos serviços de TI, da organização?" considera a resposta "utilizadores" se forem partilhados dados dos utilizadores e que possam identificar a identidade dos mesmos, considera a resposta "negócio" se forem partilhados decorrentes do negócio da organização mas que não permitam identificar os utilizadores e em "estatísticos" se a organização partilhar dados dos utilizadores mas na situação em que estes dados não permitem identificar o utilizador a que estes se referem;

- a questão "A organização tomou todas as medidas necessárias para a preservação da privacidade da informação dos utilizadores?" é codificada em "sim" se a

organização detiver meios para controlar e verificar utilização dos dados dos utilizadores e em "não" se a organização não detiver essa capacidade; entendendo-se por controlar, no contexto desta questão, a capacidade verificar quem e quais os serviços que acedem a dados, qual o motivo do acesso e capacidade de restringir acesso a dados dos utilizadores no âmbito dos SI da própria organização independentemente das TI utilizadas e dos modelos de alojamento utilizados;

- no caso da questão "A organização é responsável pela informação dos clientes?" é pretendida a resposta "Sim" se todos os dados disponibilizados pelos utilizadores forem alvo de gestão e controlo de privacidade de informação por parte da organização e em "não" se existir pelo menos um serviço, na organização, em que os dados e conteúdos disponibilizados pelos utilizadores sejam da responsabilidade dos mesmos;

- a questão "A organização tem procedimentos de manutenção de dados?" procura verificar se as organizações detêm procedimentos implementados nos SI para manter a consistência, fiabilidade, segurança e atualidade dos dados dos utilizadores a que se dará a resposta "sim" em caso afirmativo e "não" em caso negativo;

- a questão "Existe, na organização, um responsável pelos dados dos utilizadores?" procura verificar se existe alguma entidade, departamento ou colaborador, que tenha como funções garantir que os processamentos de dados subscrevem todas as regras de privacidade de informação implementadas na organização a que será dada a resposta "sim" em caso de existência e não no caso de não existir;

- a questão "A organização controla todos os serviços de terceiros que acedem a dados partilhados?" refere-se à capacidade da organização decidir quais os serviços de

terceiros têm acesso aos dados partilhados e de a qualquer momento fechar esse acesso, em caso afirmativo será dada a resposta “sim” em caso negativo ”não”;

- a questão “A organização tem implementados procedimentos para assegurar a regra de eliminação total dos dados dos utilizadores?” caso as organizações tenham implementados este tipo de procedimentos, em todos os seus SI, será codificada a resposta “sim”, caso contrário será codificado como “não”;

- a questão “A organização tem implementados procedimentos para assegurar a regra de portabilidade dos dados dos utilizadores?” caso, as organizações, detenham procedimentos implementados que permitam fornecer ao utilizador todos os seus dados em formato legível, será codificada a resposta “sim”, caso contrário será codificado como “não”;

- a questão “A organização armazena os dados dos seus utilizadores apenas pelo tempo necessário para o processamento para o qual foram recolhidos?” é codificado com a resposta “sim” caso todos os dados dos utilizadores sejam eliminados no final do processamento ou no final do prazo legal, para o qual a organização é obrigada a armazenar os dados, e é codificada com a resposta “não” em caso negativo;

- à questão “A organização, pede o consentimento explicito, aos utilizadores, para processar os seus dados noutros processamentos para alem dos que levaram à recolha dos dados?” é dado o código de resposta “sim” caso, a organização, utilize os dados dos utilizadores, pedindo o seu consentimento, para outros processamentos, como o caso de processamentos de marketing ou outros, e é codificada a resposta com “não” caso não se verifique o pedido de consentimento.

A tabela 3, é gerada, com os resultados das opiniões dos entrevistados, no que respeita ao impacto que causará às suas organizações a implementação das novas regras de privacidade de dados da EU. No primeiro ponto, impacto tecnológico, é avaliado, pelo entrevistado, o impacto que terá nos SI da organização, a introdução das novas regras. Com este ponto, o estudo procura entender se os atuais SI terão alterações a nível de desenvolvimento significativas com a introdução das novas regras. No ponto 2, impacto financeiro, o estudo pretende entender se a implementação das novas regras terá impacto financeiro nas organizações, tanto pelos custos de desenvolvimento em termos de SI como de custos derivados da alteração de processos de negócio ou de implementação de novos. No ponto 3, impacto no negócio, procura-se entender se a implementação das novas regras de privacidade irão modificar ou acrescentar novos processos ao negócio das organizações. Nestes três pontos, as respostas, com base na opinião dos entrevistados sobre a realidade das suas organizações, serão codificadas com as respostas "baixo", se o impacto for baixo, "médio" se o impacto for de um nível considerável e "alto" se o impacto for significativo para a realidade da organização. Relativamente ao ponto 4, tempo de implementação das novas regras nos SI da organização, será codificada a resposta em "curto" se o tempo de implementação for inferior a 1 mês, será codificada de "médio" se o custo de implementação for de um mês a um ano e será codificada como "alto" se o tempo de implementação for superior a um ano.

Ainda na entrevista, na opinião dos entrevistados, com base na sua experiência profissional e no estado atual das suas organizações relativamente à privacidade de informação, foram recolhidos os fatores que potencialmente possam ter impacto e inibir a implementação das novas regras de privacidade nas suas organizações.

7.5. RESULTADOS

Com a análise dos dados verificou-se que o conhecimento sobre a DEPD e da sua reforma é reduzido na maioria organizações estudadas com exceção do setor das telecomunicações e de serviços de TI. Relativamente à reforma das diretivas, verifica-se que em todos os setores de atividade dos entrevistados é possível a eliminação da totalidade de dados dos utilizadores e, também, é possível extrair a totalidade dos dados dos utilizadores para fornecimento em formato legível. No entanto, no que respeita à regra de recolha mínima de dados necessários para o processamento dos dados dos utilizadores apenas as organizações do setor de serviços *cloud* e da aviação cumprem, atualmente, a regra. No que respeita à regra de armazenamento dos dados dos utilizadores pelo tempo mínimo necessário para o processamento solicitado, apenas as empresas dos setores de telecomunicações e de serviços de TI cumprem a regra de momento. A regra de processamento de dados apenas com o consentimento explícito dos utilizadores é cumprida, atualmente, pela organização de telecomunicações e pela organização de serviços de TI. Na organização do setor da saúde, os dados recolhidos são utilizados, posteriormente, para processamento estatístico sem que seja possível identificar o utilizador proprietário dos dados enquanto na maioria das restantes organizações os dados são utilizados para fins comerciais ou de marketing da própria organização.

No que respeita às TI das organizações, a maioria, das organizações estudadas, utiliza somente recursos próprios ou em regime de alojamento externo, sem partilha de recursos. No entanto, as organizações das áreas das telecomunicações e aviação utilizam, também, *cloud computing* considerando em ambos os casos como tendo tendência a aumentar a utilização deste modelo de computação. A organização de

serviços TI, especializadas tecnologias de CRM, é a única a usar somente recurso em regime de *cloud computing*. Neste modelo, *cloud computing*, as organizações sentem que são tomadas todas as medidas de segurança relativas à partilha de infra-estrutura de suporte às suas aplicações e dados com outras aplicações de outras organizações e relativas à exposição dos seus SI a acessos indevidos. Esta segurança que as organizações sentem, deve-se à segurança que os prestadores de serviços de *cloud computing* transmitem com o cumprimento de diversos protocolos de segurança tais como a ISO 27001.

A utilização de tecnologias *Web* 2.0 é uma realidade, em todas as áreas de atividade consultados. As aplicações *Web* 2.0 são utilizadas internamente, para funcionamento das próprias organizações, e externamente, via acesso pela Internet, pelos utilizadores em geral.

A disponibilização pública de conteúdos inseridos pelos utilizadores, apenas, surge nas organizações do setor da comunicação social e de serviços TI (CRM), estando nas restantes organizações fechado o acesso publico a dados dos utilizadores. As organizações que partilham dados publicamente, partilham conteúdos inseridos pelos próprios utilizadores, enquanto as organizações que partilham dados com outras organizações para além dos dados dos utilizadores disponibilizam ainda dados estatísticos e dados decorrentes do seu próprio negócio.

A privacidade de informação é uma preocupação da maioria das organizações que consideram os dados dos seus utilizadores como sensíveis ou muito sensíveis, tendo a generalidade das organizações implementados processos de auditoria e de controlo de acesso aos dados dos seus utilizadores. Na sequência da protecção de dados e da

sensibilidade destes, as organizações que consideram os dados dos seus utilizadores muito sensíveis têm um responsável ou departamento responsável pela segurança e proteção de dados. No entanto as palavras do entrevistado da organização de serviços TI de CRM que diz "… na fase de desenvolvimento do serviço, as preocupações não são com a segurança mas sim com as funcionalidades da aplicação" apontam para uma preocupação apenas nas fases após a implementação das soluções.

O controlo dos acessos, de serviços de terceiros, que acedem aos dados das organizações, apenas não sucede nas organizações que disponibilizam publicamente, nas suas aplicações *Web* 2.0, na Internet. Todas as outras organizações conseguem controlar quais os serviços externos à organização acedem aos seus dados. Segundo o entrevistado da área da saúde que afirma que "… todos os serviços externos que acedem à nossa organização utilizam canais dedicados por VPN para o fazerem…", assegurando o controlo dos serviços disponibilizados a terceiros.

Os procedimentos, para cumprimento das novas regras europeias de privacidade de dados, respeitantes à duração do armazenamento de dados e à solicitação de consentimento para processamentos posteriores não se encontram já implementados em nenhuma das organizações consultadas. Relativamente ao armazenamento de dados, o entrevistado do setor da comunicação social diz que "os dados são armazenados indefinidamente não porque estes sejam usados atualmente para outro tipo de processamento, mas existindo a possibilidade de os usar futuramente leva-nos a não os eliminar" revela que as organizações têm em conta o uso de dados para outros processamentos e que assim não consideram a sua eliminação. Quanto às regras de eliminação total de dados e da portabilidade de dados apenas a organização

do setor das telecomunicações já detém o procedimento para as aplicar. Segundo o entrevistado do setor de serviços TI (CRM) que revela que "… na implementação dos sistemas de CRM é possível disponibilizar o procedimento para eliminação total dos dados mas tal nunca nos foi requisitado pelos clientes", não existe preocupação na implementação deste tipo de procedimentos.

A implementação das novas regras tem, na generalidade das organizações um impacto baixo, quer em termos de impacto tecnológico, seja ao nível de recursos de TI quer seja pelo esforço de desenvolvimento dos próprios procedimentos; quer em termos financeiros, dado que os custos de desenvolvimento são baixos e os recursos de TI já existentes são considerados suficientes para suportar as alterações; em termos de negócio as novas regras não irão afectar os processos já existentes passando apenas pela adição de novos processos.

Na maioria das organizações, os entraves à implementação das novas regras são considerados poucos. No entanto, a eliminação dos dados que possam ter sido partilhados publicamente ou a serviços de terceiros poderá ser difícil uma vez que as organizações não controlam o destino que é dado aos dados por outras organizações. Esta situação, torna-se mais complicada, dado, que por imperativos de negócio é necessário haver transferência de dados entre organizações, incluindo organizações que possam estar fora de território europeu e que assim não são abrangidas pela diretiva europeia e pela sua reforma. De acordo com o entrevistado do setor da aviação, que afirma que "no processo de reservas é necessário enviar os dados dos utilizadores tanto para a plataforma externa de reservas como para as autoridades no destino", revelando a necessidade de partilha de dados privados dos utilizadores,

salientando, no entanto, que deveria ser possível controlar o destino que é tomado por esses dados.

8. CONCLUSÃO

Este estudo pôde concluir, que apesar da possibilidade de cumprir as novas regras de privacidade de dados ser uma realidade em todas as organizações consultadas, apenas uma minoria já detém procedimentos para aplicar parte destas mesmas regras.

A implementação das regras poderá ser relativamente fácil, no entanto, quando as regras abrangem dados que são transferidos para fora dos SI das organizações estas tornam-se mais complicadas de implementar. O controlo dos dados fora das organizações não é possível e não é fornecido conhecimento, às próprias organizações pelos serviços externos, sobre os processamentos que são efetuados pelos dados partilhados entre as organizações. A ausência de uma entidade que faça o controlo dos dados entre organizações e que assegure o cumprimento das regras é uma das causas para este desconhecimento. Verificou-se, ainda, que a privacidade de informação e a segurança de dados não está presente em todo o ciclo de vida do desenvolvimento das aplicações. Por outro lado, poderão existir processos de negócio impeditivos da implementação das novas regras de privacidade de dados. Ainda como fatores inibidores, surgem a ausência de um responsável pela segurança de dados nas organizações e a ausência de preocupação com a privacidade de informação em todo o ciclo de vida de desenvolvimento dos SI das organizações. O processamento, posterior, de dados para fins estatísticos ou comerciais poderá, igualmente, ser um fator inibidor.

Este estudo foi efetuado, com o objectivo de fornecer possíveis fatores que possam impossibilitar a implementação das novas regras europeias de privacidade de dados e

para que possa no futuro contribuir para a descoberta de soluções para a eliminação destes fatores.

O estudo aqui apresentado, teve, como principal limitação, o número reduzido de organizações consultadas. A consulta de mais organizações, poderia ter enriquecido a investigação com mais cenários de aplicações e de particularidades de negócio que poderiam levar a mais fatores inibidores da implementação das novas regras de privacidade de dados, bem como a uma noção mais abrangente da atenção que é dada à privacidade de informação e à protecção dos dados dos utilizadores.

Numa possível tese de doutoramento, o presente estudo, poderia contribuir com informação e dados que possam levar a um modelo de avaliação do nível das organizações quanto à privacidade de informação, criado e testado através de uma aproximação quantitativa.

9. REFERÊNCIAS BIBLIOGRÁFICAS

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinsky, A., et al. (2010). Clearing the clouds away from the true potential and obstacles posed by this computing capability. *Comunicationsof the ACM*, 50-58.

Bélanger, F., & Crossler, R. E. (2011). Privacy In The Digital Age: A Review Of Privacy Research in Information Systems. *MIS Quarterly, 35*(4), 1017.

Boulos, M. N., & Wheeler, S. (2007). The emerging Web 2.0 social software: an enabling suite of sociable technologies in health and health care education. *Health Information and Libraries Journal*, 2–23.

Chen, J., & Wang, L. (2011). Cloud Computing 2011. *Journal of Computer andSystem Sciences*.

Comissão Europeia. (1995). Directiva 95/46/CE do Parlamento Europeu e do Conselho. *Jornal Oficial das Comunidades Europeias*.

Comissão Europeia. (1997). Directiva 97/66/CE do Parlamento Europeu e do Conselho. *Jornal Oficial das Comunidades Europeias*, L24/1-L24/8.

Comissão Europeia. (2002). Directiva 2002/58/CE do Parlamento Europeu e do Conselho. *Jornal Oficial das Comunidades Europeias*, 201/37-201/47.

Comissão Europeia. (2010). *European Commission sets out strategy to strengthen EU data protection rules*. Obtido em 30 de Novembro de 2011, de Europa - EU: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462

Comissão Europeia. (2011). *Data Protection: Europeans share data online, but privacy concerns remain – new survey*. Obtido em 03 de 12 de 2011, de Europa - EU: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/742&format=HTML&aged=0&language=EN&guiLanguage=en

Comissão Europeia. (2011). *Stronger data protection rules at EU level: EU-Justice Commissioner Viviane Reding and German Consumer Protection Minister Ilse Aigner join forces*. Obtido em 30 de Novembro de 2011, de Europa - EU: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/762&format=HTML&aged=0&language=EN&guiLanguage=en

Comissão Europeia. (2012). *Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados).* Bruxelas.

ComputerWorld. (2011). *Reforma europeia na protecção de dados coloca pressão sobre empresas estrangeiras*. Obtido em 14 de Novembro de 2011, de ComputerWorld.com.pt: http://www.computerworld.com.pt/2011/11/11/reforma-europeia-na-proteccao-de-dados-coloca-pressao-sobre-empresas-estrangeiras/

Dhillon, G. (2003). Data and information security. *Journal of Database Management, 14*(2), p. 1.

Dhillon, G. (2004). Realizing benefits of an information security program. *Business Process Management Journal, 10*, p. 260.

Dhillon, G. (2007). *Principles of Information Systems Security: text and cases.* New York: Wiley and Sons.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information. *Information Systems Journal, 16*, pp. 293-314.

European Network and Information Security Agency. (2012). *Study on data collection and storage in the EU.*

Harauz, J., Kaufman, L. M., & Potter, B. (Jul-Ago de 2009). Data Security in the World of Cloud Computing. *IEEE SECURITY & PRIVACY, 7*(4), 61 - 64.

Harison, E. (2010). Who owns enterprise information? Data ownership rights in Europe and the U.S. *Information & Management, 47*(2), pp. 102-108.

Kandukuri, B. R., Paturi, R. V., & Rakshit, A. (2009). Cloud Security Issues. *Services Computing, 2009. SCC '09. IEEE International Conference on*, (pp. 517 - 520).

Kormaris, G., & Spruit, M. (2010). Bridging the gap between Web 2.0 Technologies and Social Computing Principles.

Kosta, E., Dumortier, J., & Graux, H. (2012). *Study on data collection and storage in the EU.* European Network and Information Security Agency. European Network and Information Security Agency.

Lee, S. M., Kim, T., Noh, Y., & Lee, B. (2010). Success factors of platform leadership in web 2.0 service business. *Springer-Verlag*.

Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). Digital Footprints: Online Identity Management and Search in the Age of Transparency. *PewResearchCenter Publications*.

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly, 10*(1), p. 5.

Musser, J. (2006). *Web 2.0 Principles and Best Practices.* O'Reilly Radar.

Quaresma, B., Bessani, A., & Sousa, P. (s.d.). *Melhorando a Disponibilidade e Confidencialidade das Clouds de Armazenamento.*

Shulman, A. (2011). *UK's New Cyber Security Strategy Does Not Help Secure The Individual*. Obtido em 3 de Dezembro de 2011, de Business Computing World: http://www.businesscomputingworld.co.uk/uks-new-cyber-security-strategy-does-not-help-secure-the-individual/

Soghoian, C. (17 de Agosto de 2009). Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era. *J. on Telecomm. and High Tech.*, 359-424.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), pp. 1-11.

Takabi, H., Joshi, J. B., & Ahn, G.-J. (2010). Security and Privacy Challenges in Cloud Computing Environments. *Security & Privacy, IEEE, 8*(6), 24-31.

Toal, P. (Abril de 2011). Information Security: A Conceptual Architecture Approach. *Oracle White Paper*.

Tumulak, D. (2010). *Enterprise Data Protection – A Security Strategy For Improving Business Processes And Reducing Data Losses*. Obtido em 3 de Dezembro de 2011, de Business Computing World: http://www.businesscomputingworld.co.uk/enterprise-data-protection-a-security-strategy-for-improving-business-processes-and-reducing-data-losses/

Zimmer, M. (2008). The Externalities of Search 2.0: The Emerging Privacy Threats when the Drive for the Perfect Search Engine meets Web 2.0. *First Monday, 13*, 3.

ANEXOS

A. ENTREVISTA

Neste anexo, são apresentadas as principais questões a serem focadas nas entrevistas aos colaboradores das organizações

- **Directivas Europeias de privacidade de dados**
    a. Tem conhecimento da directiva europeia de privacidade de dados?
    b. Tem conhecimento da reforma à directiva europeia de privacidade de dados e das suas novas regras?
- **Utilização de Tecnologias Cloud**
    a. A sua organização utiliza tecnologias *cloud computing* e/ou *Web 2.0*? Presta serviços *cloud*?Que tipo de serviços?
    b. Utiliza recursos próprios (Housing) ou baseado em Cloud para armazenamento de dados?
    c. Os recursos utilizados para alojamento de dados são partilhados com outras organizações?
    d. Que tipo de medidas são utilizadas para garantir a segurança dos dados (Ex: ISO27001, processos de auditoria)?
        i. Considera que são as suficientes?
    e. A sua organização é responsável pela manutenção da informação dos clientes?
    f. Tem processos para manutenção regular dos dados dos clientes? Os dados dos seus clientes estão actualizados? Com que periodicidade?
    g. Existe alguém na organização responsável pela segurança dos dados dos clientes (Controlador/Segurança de dados)?
    h. As aplicações da organização utilizam/partilham dados via Web?

i. São partilhados dados com outros serviços ?

j. Que tipo dados são partilhados? Pessoais/Comerciais/Empresariais.

k. Consegue controlar os serviços que acedem a dados partilháveis via Web pela organização.

- **Novas Regras**

a. A sua organização consegue disponibilizar os dados para que possam ser transportados para outro prestador de serviço?

i. A organização já detêm um processo para o fazer ?

b. Considera que a sua organização ou a organização contratada detém capacidade para eliminar os dados dos seus clientes, inclusive os que possam ter sido disponibilizados via www? (Com excepção dos obrigatórios manter por questões de legais, ex: facturação)

i. E os dados disponibilizados a outros serviços?

ii. Detém um processo para o fazer ?

c. Tem contratualizado o apagar de informação com os clientes ou outros serviços que possam recolher dados da sua organização?

i. Detém um processo para o fazer ?

d. Mantém os dados de clientes/utilizadores para questões de histórico?

i. Estes são eliminados quando o cliente/utilizador cessa o serviço na sua organização

e. É recolhida informação adicional para além do estritamente necessário para a execução do processamento/serviço pedido pelo utilizador?

- **Opinião**

a. Qual a sua posição e da sua organização quanto à privacidade de dados quer da organização quer de clientes? É um foco/preocupação? Ou uma obrigação/dever?

b. Qual seria o nível de impacto na sua organização a implementação das regras mencionadas na introdução (A nível de Negócio/Financeiro/Tecnológico ?

c. Tendo em conta as 4 novas regras referidas na introdução, o que pensa delas e da sua implementação na sua organização

    i. E em Portugal/Europa ?

B. TABELAS

1. Tabela 1 - Conhecimento e Implementação DEPD

Sector Actividade	O entrevistado detém conhecimento sobre a DEPD?	O entrevistado detém conhecimento sobre a reforma da DEPD?	É possível a eliminação total dos dados dos utilizadores?	É possível a portabilidade dos dados dos utilizadores?	São recolhidos os dados mínimos necessários para o processamento?	Os dados, dos utilizadores, recolhidos são armazenados apenas pelo tempo necessário para efetuar o processamento para o qual foram recolhidos?	Todos os processamentos efetuados sobre os dados dos utilizadores têm o seu consentimento explícito?
Comunicação Social	Não	Não	Sim	Sim	Não	Não	Não
Serviços Cloud	Não	Não	Não	Não	Não	Não	Não
Telecomunicações	Sim	Não	Sim	Sim	Não	Não	Sim
Aviação	Não	Não	Não	Não	Não	Não	Não
Serviços TI (CRM)	Não	Não	Sim	Sim	Não	Não	Não
Serviços TI	Sim	Não	Sim	Sim	Não	Não	Sim
Saúde	Não	Não	Sim	Não	Não	Sim	Não

Tabela 1 - Conhecimento e implementação da directiva europeia de protecção de dados

2. Tabela 2 - Estado actual de utilização de TI e privacidade de informação

Sector de Actividade	São utilizados recursos internos de TI na organização?	A organização utiliza recursos TI no modelo de *cloud computing*?	A organização presta serviços de *cloud computing*?	A organização utiliza TI *Web* 2.0?	A organização presta serviços de TI *Web* 2.0?	A organização partilha conteúdos disponibilizados pelos utilizadores publicamente?	A organização partilha dados dos seus utilizadores com serviços TI de outras organizações?	Quais os tipos de dados partilhados pelos serviços de TI, da organização?	A organização tomou todas as medidas necessárias para a preservação da privacidade da informação dos utilizadores?	A organização é responsável pela informação dos clientes?	A organização tem procedimentos de manutenção de dados?	Existe, na organização, um responsável pelos dados dos utilizadores?	A organização controla todos os serviços de terceiros que acedem a dados partilhados?	A organização tem implementados procedimentos para assegurar a regra de eliminação total dos dados dos utilizadores?	A organização tem implementados procedimentos para assegurar a regra de portabilidade dos dados dos utilizadores?	A organização armazena os dados dos seus utilizadores apenas pelo tempo necessário para o processamento para o qual foram recolhidos?	A organização, pede o consentimento explicito, aos utilizadores, para processar os seus dados noutros processamentos para alem dos que levaram à recolha dos dados?
Comunicação Social	Sim	Não	Não	Sim	Sim	Sim	Não	utilizadores	Sim	Sim	Não	Não	Não	Não	Não	Não	Não
Serviços Cloud	Sim	Sim	Sim	Sim	Sim	Não	Não		Sim	Sim	Sim	Sim	Sim	Não	Não	Não	Não
Telecomunicações	Sim	Sim	Sim	Sim	Sim	Não	Não		Sim	Não	Sim	Não	Sim	Sim	Sim	Não	Não
Aviação	Sim	Sim	Não	Sim	Sim	Não	Sim	Negócio/ utilizadores	Sim	Sim		Sim	Não	Não	Não	Não	Não
Serviços TI (CRM)	Sim	Sim	Não	Sim	Sim	Sim	Sim	utilizadores	Não	Sim	Sim	Não	Não	Sim	Não	Não	Não
Serviços TI	Sim	Não	Não	Sim	Sim	Não	Não		Sim	Sim	Não	Não	Sim	Não	Não	Não	Não
Saúde	Sim	Não	Não	Sim	Sim	Não	Sim	Estatísticos	Sim	Sim	Não	Sim	Sim	Não	Não	Não	Não

Tabela 3 - Estado actual das organizações relativo à utilização de TI e protecção da privacidade de dados

3. Tabela 3 - Impacto da implementação das novas regras de privacidade de dados

Sector de Actividade	Impacto Tecnologico	Impacto Financeiro	Impacto Negócio	Tempo de implementação
Comunicação Social	Baixo	Baixo	Baixo	Curto
Serviços Cloud	Médio	Médio	Baixo	Médio
Telecomunicações	Baixo	Baixo	Baixo	Médio
Aviação	Baixo	Baixo	Baixo	Médio
Serviços TI (CRM)	Baixo	Baixo	Baixo	Curto
Serviços TI	Baixo	Baixo	Baixo	Curto
Saúde	Baixo	Baixo	Baixo	Médio

Tabela 4 - Impacto da implementação das novas regras de privacidade de dados